What is claimed is:

1. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

implementing a telemetry interlock which limits any communications between the ED and the IMD over the telemetry channel;

releasing the telemetry interlock by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD;

authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.

2. The method of claim 1 wherein the ED and the IMD are authenticated to one another using public key cryptography by:

authenticating the IMD to the ED when the ED encrypts a first message with a public key having a corresponding private key expected to be possessed by the IMD, transmits the encrypted first message over the telemetry channel to the IMD, and receives in response a message from the IMD derived from the first message which thereby evidences possession of the corresponding private key by the IMD; and,

authenticating the ED to the IMD when the IMD encrypts a second message with a public key having a corresponding private key expected to be possessed by the ED, transmits the encrypted second message over the telemetry channel to the ED, and

receives in response a message from the ED derived from the second message which thereby evidences possession of the corresponding private key by the ED.

3. The method of claim 2 wherein the message derived from the first message includes the first message and wherein the message derived from the second message includes the second message.

4. The method of claim 2 wherein the first and second messages include random numbers generated by the ED and IMD, respectively.

5. The method of claim 2 wherein the first and second messages include identity codes for the ED and IMD, respectively.

6. The method of claim 2 wherein the messages derived from the first and second messages and which are transmitted by the IMD and ED, respectively, are encrypted using the public keys of the ED and IMD, respectively.

7. The method of claim 2 wherein the message derived from the first message which is transmitted by the IMD includes the second message.

8. The method of claim 1 further comprising encrypting communications between the ED and IMD during the data communications session.

9. The method of claim 2 further comprising encrypting communications between the ED and IMD during the data communications session with secret key cryptography, wherein the secret key data communications session is established by one of either the ED or the IMD transmitting to the other of either the ED or the IMD a secret session key encrypted by the latter's public key.

10. The method of claim 1 wherein one of either the ED or the IMD is designated as a session instigator and the other of the ED or IMD is designated as a session recipient, the ED and the IMD are authenticated to one another using public key cryptography, and authentication is accomplished by:

the instigator encrypting a first message with a public key having a corresponding private key expected to be possessed by the recipient, wherein the first message includes an identity code for the instigator and a random number R_A,

the instigator transmitting the encrypted first message over the telemetry channel to the recipient;

the recipient decrypting the first message with its private key, looking up a public key having a corresponding private key expected to be possessed by the instigator using the identity code contained in the first message, and encrypting a second message with the public key of the instigator, wherein the second message includes an identity code for the recipient, the random number R_A, and a second random number R_B;

the recipient transmitting the encrypted second message over the telemetry channel to the instigator;

the instigator decrypting the second message with its private key corresponding to the public key used to encrypt the second message and verifying that the second message contains R_A to thereby authenticate the recipient;

the instigator encrypting a third message derived from the second message with the public key of the recipient, wherein the third message includes the random number R_B;

the instigator transmitting the encrypted third message over the telemetry channel to the recipient; and,

the recipient decrypting the third message with its private key corresponding to the public key used to encrypt the third message and verifying that the third message contains R_B to thereby authenticate the instigator.

11. The method of claim 10 further comprising encrypting communications between the instigator and the recipient during the data communications session with secret key cryptography, wherein the secret key data communications session is established by the instigator transmitting to the recipient a secret session key encrypted by the recipient's public key.

12. The method of claim 11 wherein the secret session key is contained in the third message transmitted by the instigator.

13. The method of claim 1 wherein the ED and the IMD are authenticated to one another using secret key cryptography by:

authenticating the IMD to the ED when the ED transmits a first message to the IMD over the telemetry channel and receives in response a message derived from the first message which is encrypted by a secret key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD transmits a second message to the ED over the telemetry channel and receives in response a message derived from the second message which is encrypted by a secret key expected to be possessed by the ED.

14. The method of claim 1 wherein, after a data communications session ends, the telemetry interlock is re-activated to limit communications over the telemetry channel until the telemetry interlock is again released.

15. The method of claim 1 wherein no communications between the ED and IMD are allowed to occur until the telemetry interlock is released.

16. The method of claim 1 wherein a data communications session over the telemetry channel can be established which allows transmission of data from the IMD to the ED if the telemetry interlock is not released, but programming of the IMD by the ED cannot be performed unless the telemetry interlock is released.

17. The method of claim 1 wherein the telemetry channel is a far-field radio-frequency communications link.

18. The method of claim 1 wherein the telemetry channel includes an internet link.

19. The method of claim 1 wherein the short-range communications channel is an inductive communications link between the IMD and another device.

20. The method of claim 1 wherein the short-range communications channel is a switch within the IMD which is actuated by a magnet held in close proximity to the IMD to thereby release the telemetry interlock.

21. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

implementing a telemetry interlock which is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD; and,

limiting data communications between the IMD and ED over the telemetry channel until the telemetry interlock has been released.

22. The method of claim 21 wherein, after a data communications session over the telemetry channel ends, the telemetry interlock is re-activated to limit communications over the telemetry channel until the telemetry interlock is again released.

23. The method of claim 21 wherein no communications between the ED and IMD are allowed to occur over the telemetry channel until the telemetry interlock is released.

24. The method of claim 21 wherein a data communications session over the telemetry channel can be established which allows transmission of data from the IMD to the ED if the telemetry interlock is not released, but programming of the IMD by the ED cannot be performed unless the telemetry interlock is released.

25. The method of claim 21 wherein the short-range communications channel is an inductive communications link between the IMD and another device.

26. The method of claim 21 wherein the short-range communications channel is a switch within the IMD which is actuated by a magnet held in close proximity to the IMD to thereby release the telemetry interlock.

27. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD has been authenticated to the ED.

28. The method of claim 27 further comprising:

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.

29 The method of claim 28 wherein the ED and the IMD are authenticated to one another using public key cryptography by:

authenticating the IMD to the ED when the ED encrypts a first message with a public key having a corresponding private key expected to be possessed by the IMD, transmits the encrypted first message over the telemetry channel to the IMD, and receives in response a message from the IMD derived from the first message which thereby evidences possession of the corresponding private key by the IMD; and,

authenticating the ED to the IMD when the IMD encrypts a second message with a public key having a corresponding private key expected to be possessed by the ED, transmits the encrypted second message over the telemetry channel to the ED, and receives in response a message from the ED derived from the second message which thereby evidences possession of the corresponding private key by the ED.

30. The method of claim 28 wherein the ED and the IMD are authenticated to one another using secret key cryptography by:

authenticating the IMD to the ED when the ED transmits a first message to the IMD over the telemetry channel and receives in response a message derived from the first message which is encrypted by a secret key expected to be possessed by the IMD;

authenticating the ED to the IMD when the IMD transmits a second message to the ED over the telemetry channel and receives in response a message derived from the second message which is encrypted by a secret key expected to be possessed by the ED.

31. A method for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the ED has been authenticated to the IMD.

32. A system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

means for implementing a telemetry interlock which limits any communications between the ED and the IMD over the telemetry channel;

means for releasing the telemetry interlock by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD;

means for authenticating the IMD to the ED when the ED receives a message from the IMD evidencing use of an encryption key expected to be possessed by the IMD;

means for authenticating the ED to the IMD when the IMD receives a message from the ED evidencing use of an encryption key expected to be possessed by the ED; and,

means for allowing a data communications session between the IMD and ED over the telemetry channel to occur only after the IMD and ED have been authenticated to one other.

33. A system for enabling secure communications between an implantable medical device (IMD) and an external device (ED) over a telemetry channel, comprising:

means for implementing a telemetry interlock which is released by transmitting an enable command to the IMD via a short-range communications channel requiring physical proximity to the IMD; and,

means for limiting data communications between the IMD and ED over the telemetry channel until the telemetry interlock has been released.

34. The system of claim 33 wherein the short-range communications channel is an inductive communications link between the IMD and another device.

35. The system of claim 33 wherein the short-range communications channel is a switch within the IMD which is actuated by a magnet held in close proximity to the IMD to thereby release the telemetry interlock.